Sanford Morganstein <Sandy@TechnologyCorp.net> on 01/25/2002 06:46:06 PM

Please respond to Sandy@TechnologyCorp.net

To: vss@FEC
cc:

Subject: Comments on Draft VSS standards

Illinois Information Technology Corporation respectfully submits its comments on the Second Draft Of The Revisions To The 1990 National Voluntary Performance Standards For Computerized Voting Systems And The First Draft Of The Revisions To The 1990 National Test Standards.

We are concurrently sending a paper copy by US Express Mail. We hope that your version of Microsoft Word is compatible with ours and that we have no compatibility or formatting issues.

If such issues do exist, we would be most pleased to send you a copy in Adobe .pdf format at your request.

Thank you for your consideration.

Sanford J. Morganstein
847-426-1010

- Comments on Draft VSS standards.doc

January 25, 2002

Ms. Penelope Bonsall
Director, Office of Election Administration
Federal Election Commission
999 E. Street, N.W.
Washington, D.C. 20463

Dear Ms. Bonsall:

Illinois Information Technology Corporation respectfully submits its comments on the *Second Draft Of The Revisions To The 1990 National Voluntary Performance Standards For Computerized Voting Systems And The First Draft Of The Revisions To The 1990 National Test Standards*. Throughout our comments we refer to this document as the "*Draft VSS Standards.*" We base our comments on the Adobe .pdf document found at the website referenced at www.fec.gov/elections.html. In some cases we refer to comments made by other commentators. We note that those comments had been posted on the website www.wote.org but as of this writing we cannot find any comments on the *Draft VSS Standards* at that website. We trust that our reference to such third party comments is considered with the understanding that we believe those comments to have indeed been made by the quoted commentators. We consequently do not vouch for the accuracy of those quotations.

As requested in the notice in the Federal Register, our comments reference specific sections of the *Draft VSS Standards*. Where possible, our comments regarding specific content are accompanied by specific suggestions for alterations to language or technical specifications. We are submitting our comments concurrently via e-mail to vss@fec.gov and via US mail. Our return address is:

Illinois Information Technology Corp.
14N880 Lac du Beatrice Dr.
W. Dundee, IL 60118

and this commentator can be reached by e-mail at:

Sandy@TechnologyCorp.net

About our company

Illinois Information Technology Corporation is an intellectual property consulting firm. We have been retained from time to time as experts on intellectual property matters, have testified in federal court on these matters and we have also managed intellectual property portfolios on behalf of clients. Our interest comes in part from our work in intellectual property but we view this field as important to our nation and we may consider entering this field with products of our own in the future. At present, we make no products dealing with elections or election administration.

As requested in the notice in the Federal Register, we respectfully submit that we are willing to present testimony to the Commission if requested to do so.

General Comments

As the *Draft VSS Standards* points out, feedback to voters, whether that feedback be for overvote, undervote or other situations, is important for ensuring that a ballot accurately expresses a voter's intent. We read the *Draft VSS Standards* and see the important feedback notion specified from the perspective of **existing** marksense, punchcard and DRE systems. Since feedback is so important, and since feedback from existing systems has often been found wanting, we believe it is reasonable to expect that innovations will appear that are difficult to view from these historical and therefore limited perspectives. We spend the major part of our commentary proposing changes to language that we believe can leave important room for new, accurate and trustworthy election systems that employ feedback and audit trails, secrecy and privacy. We also feel that our comments permit more room for innovation without sacrificing precision and without introducing ambiguity in the standards.

Comments on the Overview § Revised Performance Features

The Draft VSS Standards contains the following section:

> "**Feedback to Voter:** Performance requirements are defined for DRE systems and for paper-based precinct-based systems in order to provide direct feedback to the voter that indicates when an undervote or overvote is detected."

The quoted paragraph is found as the second bullet item. The only other place "feedback" to voters is specifically found is in § **2.4.3.2.2 Precinct Count Paper-Based Systems**. We quote that section (subparagraph (a)): "Provide feedback to the voter that identifies specific contests or ballot issues for which an overvote or underrate [sic] is detected." This implies that feedback to the voter on undervote or overvote situations only occurs in paper based systems that have precinct count systems. As we will point out below, crucial voter feedback can be provided on paper-based systems (punchcard, marksense or other) that do not have in-precinct counters. This linkage of voter feedback to paper-based precinct-count systems is found again in § **3.2.5.1.3 Exception Handling**

(Precinct Count) subparagraphs (c) and (d).

Before providing a suggestion that gets closer to the spirit of the fundamentally important issue of voter feedback, we point out that others consider the issue of voter feedback to be of high concern, as we believe the Commission does.

At least one commentator (Peter G. Neumann, or SRI International) has said:

> "The feedback I want most is that my vote has been correctly recorded exactly as it has been cast. In electronic election systems, we need an independent voter-approved record other than what appears on the screen (for example, a paper image of what appears on the screen) that can be verified by the voter and assurably not subsequently be subjected to tampering."

Furthermore, Dr. Rebecca Mercuri, in her comments raises similar points ("One solution to the disappearing electrons problem is to require that all fully-electronic balloting systems provide a physical audit trail that is human-readable.").

We support these views and request in simple terms that the Draft VSS Standards **clearly allow for tangible feedback mechanisms in both electronic systems and mechanical or electronic ballot marking in paper-based systems.**

Nothing that we find in the Draft VSS Standards appears to be at odds with this important concept. On the other hand, there are certain sections that could be improved with a few clarifying language changes that can ensure that the spirit of "feedback" and security (*i. e.* the voter should be assured that what the voter intended or did is what will be counted) is clear in the final *VSS Standards*. The following comments address this concern and offer suggestions that we hope clarify the intent of the Commission.

Page 3 of the Overview document states:

> "Paper-based systems encompass both punchcards and optically scanned ballots. Electronic systems include a broad range of DRE systems, such as those that use touch screens and/or keyboards to record votes."

There is no direct contradiction in the quoted section, but punchcards and/or optically scanned ballots may be produced by a voter using a mechanical device, a touch screen or keyboard to **prepare** or **mark**, not necessarily to **record**, votes. Simply including touch screens and keyboards in the DRE sentence may lead to confusion. We suggest the following language:

> "Paper-based systems encompass both punchcards and optically scanned ballots. Ballots expressing the voter's intent used in such systems may be prepared manually, mechanically or electronically in secrecy by the voter in the polling place. Electronic systems include a broad range of DRE systems and magnetic output, electronic or other ballot output systems in which the voters' selections are not stored nor counted within the electronic system on which the voter marks the ballot, and may use touch screens and/or keyboards and/or other suitable input devices to mark votes."

The proposed language would also solve a problem that appears on page 6 of the Overview Document. A section entitled "Detailed Human Interface and Usability Standards" states:

> "The FEC has begun the development of the next module to the Standards, which will focus on interface and usability issues such as typography, layout, use of graphic elements, sequencing, **screen flow (for electronic systems)** [emphasis added], language simplification, and user testing."

The quoted paragraph may imply that electronic systems have screen flow and paper based systems do not. As we hoped to have clarified in our proposed language change, electronic systems encompass not only DRE systems and may have some form of countable, tangible output. Paper-based systems may use some mechanism or electronics to assist the voter in marking a ballot.

We believe that the unnecessary, and in our view, deleterious, implied restriction that feedback in paper-based systems can only be found in "in-precinct" counting systems can be improved by moving § **2.4.3.2.2 Precinct Count Paper-Based Systems** to become a new subparagraph (e) in § **2.4.3.2.1 All Paper-Based Systems**.

The rest of the paragraph on page 3 of the Overview states:

> "In addition, voting systems that use electronic ballots and transmit official vote data from the polling place to another location over a public network are now designated as Public Network DRE Voting Systems and are subject to the standards applicable to other DRE systems, and to requirements specific to systems that use public network telecommunications."

One can easily imagine a voting system consisting of punchcards that are "read" in the polling place. The data associated with these punchcards can certainly be transmitted electronically to a central tallying facility. Since the voter prepared a punchcard, it may be misleading to call such a system a "Public Network DRE Voting System." The quoted language seems to require that transmission of data collected at a polling place, whether that data be paper-based or otherwise, be classified as a Public Network DRE. Calling such systems DRE systems may cause a paper-based system to be improperly classified as a DRE system. We believe, but have no specific knowledge of cases where this is true, that some jurisdictions currently transmit precinct counted paper-based data electronically. If such systems were to be classified as DRE systems, certification of such systems would be problematic.

On a less significant, but nonetheless clarifying note, we would like to point out that transmission of data from the polling place to a central tallying facility may not take place over a *public* network. Some jurisdictions may already have, or indeed may decide to have, *private* networks.

We propose the following language and a terminal additional sentence to clarify further.

> "In addition, voting systems that use electronic ballots and transmit official vote data from the polling place to another location over an electronic network are now designated as Electronic Network DRE Voting Systems and are subject to the standards applicable to other DRE systems, and to requirements specific to systems that use electronic network telecommunications. Paper-based systems that transmit official vote data from the polling place to another location over a network are not designated as Electronic Network DRE Voting systems."

Comments on Volume I Section I § 1.51 Voting System

The last paragraph states:

> "Innovations that use a fluid understanding of system types can greatly improve the voting system industry, but only if controls are in place to integrity [sic] through the proper evaluation of the system brought for qualification."

It seems that something is missing. Might the sense you are trying to convey be:

> "Innovations that use a fluid understanding of system types can greatly improve the voting system industry, but only if controls are in place to monitor and control integrity through the proper evaluation of the system brought for qualification."

Comments on § 1.52 Paper-Based Voting System

This section has the following definition:

> "A punchcard voting system allows a voter to record votes by means of holes punched in designated voting response locations; a marksense voting system allows a voter to record votes by means of marks made in voting response locations."

We would like to point out that paper-based voting systems (both marksense and punchcard) need not be limited to "marks made in voting response locations." If these definitions are ever understood to be restrictions, innovations that build confidence, efficiency and more quality into our electoral systems may be unnecessarily stifled. Any machine readable mark on paper that correctly associates the mark with the voter's intent should come under the definition of a Paper-Based system. Here are some examples of Paper-Based systems that can associate a mark with the voter's intent:

- A mechanical or computer based system that places symbols on a paper ballot said symbols uniquely and accurately reflecting the voter's intent and having been placed by a mechanism as a result of a voter making a selection by voice, touch, keyboard or other entry.
- An Optical Character Recognition (OCR) system that accurately reads a voter's handwriting and/or printing.
- An OCR system that reads numbers that a voter writes anywhere on a ballot such number uniquely identifying the voter's intent. Such numbers have been called "punch numbers."
- A free form system used by an access-challenged or illiterate person in which the access-challenged or illiterate person writes symbols on a paper ballot such symbols uniquely and accurately identifying the voter's intent.

While the language you propose in Section 1.52 may include such cases, we propose the following language which may be more clear:

(Proposed) § 1.52 Paper-Based Voting System

> "A Paper-Based Voting System, (referred to in the initial Standards as a Punchcard and Marksense [P&M] Voting System) records votes, counts votes, and produces a tabulation of the vote count from votes cast on paper cards or sheets. A punchcard voting system allows a voter to record votes by means of holes punched on a paper ballot in a such a way that the holes unambiguously reflect the voter's selection(s); a marksense voting system allows a voter to record votes by means of marks made on a paper ballot such that those marks unambiguously reflect the voter's selection(s)."

Sections 1.54 (Public Network Direct Record Electronic (DRE) Voting System) and **1.55 (Precinct Count Voting System)** seem to contemplate public networks only. Some jurisdictions may have private networks. Since Section 1.54 is concerned about security of transmission in a *public* network, perhaps a section stating the standards for *private* network DRE Voting Systems is needed. Alternatively, if the Commission feels that security in a private network is just as problematic as security in a public network, the term "Public Network" may be replaced by "Electronic Network" in order to include both cases.

Comments on Section 2.2.7.2 DRE Standards

This general set of standards relates to access for those who have access challenges. Paragraph 4 states as follows: "4) Enables the voter to review the voter 's write-in input, edit that input, and confirm that the edits meet the voter 's intent;"

While this requirement is laudable in its intent, solutions to this problem may lead to some unintended consequences. In particular, some jurisdictions will not allow the same ballot rights to write-in candidates as they allow to candidates who have been through a petition or other legal process to be a valid candidate. The *Draft VSS Standards* have asked for no special write-in confirmations in cases where access is not a problem; consequently, there should not be any special write-in confirmation for voters with access challenges. Yes, the *Draft VSS Standards* do ask for confirmation of overvotes and undervotes for all voters and we suggest that this is the concept that should be applied for access challenged voters. For example using a punchcard system, a voter who does not have access challenges, is not given any safeguards that a name is spelled correctly or the write-in is entered in the appropriate section of the punchcard. A voter may inadvertently vote for Smith when the intent is candidate Smithe. The same logic applies to this section of the *Draft VSS Standards*. Allowing an access challenged voter to select a write-in candidate from a drop down list or allowing such a voter to spell a name could be viewed by some as elevating the status of a write-in candidate to the status of a petitioned candidate. Furthermore, consider a voter with multiple challenges. While we do not pretend to imagine all ways in which the draft requirement can be met, we note that a keyboard may not meet the draft standard for voters with multiple challenges. Requiring a keyboard or a (screen-based) facsimile thereof for a challenged voter to enter a write-in may present problems that have no solution to DRE manufacturers. This would have the consequence that no DRE can be certified that meets the needs of voters with multiple challenges.

Our recommendation, therefore, is simply to require that the standard reflect the importance of verifying that the challenged voter has indeed entered a write-in vote without further specifying that the identity of the write-in be confirmed. Our proposed language can be found below:

> "Enables the voter to review the voter's intent for write-in input, provide for the voter to change such write-in to a non-write-in vote, and confirm that entering a write-in meets the voter's intent;"

Also, paragraph 6 of this same section (**§ 2.2.7.2 DRE Standards**) provides:

> "6) Supports the use of headphones provided by the system that may be discarded after each use."

We believe that the intent of this section is the provision of sanitary conditions acceptable to the voter. One can imagine a less expensive solution consisting of **protective headphone covers** that can be discarded after each use.

Paragraph 8e of this same section (§ **2.2.7.2 DRE Standards**) has some points that may warrant reconsideration. We present our comments below each of the points we ask to be reconsidered:

> "e. For electronic image displays, permit the voter to:
> 1)Adjust the contrast settings;
>
> 2)Adjust color settings, when color is used; and…."

We note that some states require that certain types of ballots be of certain colors. Similarly, each party in a primary may have to be displayed in a different color. The quoted draft requirement may be in conflict with certain color rules.

> "3) Increase the screen font size to at least 18 points.

The problem we note here reappears in § **2.4.3.1 Common Standards.**

We note that increasing the font size on a display screen may cause some of the candidates to be hidden or moved to a part of the screen which is not in view. Visually challenged voters may not understand that they have to "scroll" or otherwise manipulate a screen to see all candidates. This requirement has the unintended consequence of discriminating against certain candidates whose ballot position is such that they disappear on an electronic screen when the font size is increased. Finally, on this point, we note that the *Draft VSS Standards* already contain a provision for audio and that audio in addition to an adequate font size set at the outset may provide enough access for the visually challenged. See § **2.3.1.2 Ballot Formatting.**

Comments on § 2.4.3.2.2 Precinct Count Paper-Based Systems

In subparagraph (a) we believe the term "underrate" is a typographical error and should be "undervote."

Comments on § 3.2.5.1.2 Exception Handling (Central Count)

The referenced section of the *Draft VSS Standards* provides for three methods of identifying an exception ballot: (outstacking, stopping, ballot marking). An additional method that facilitates exception handling could be printing a facsimile image (a copy) of the exception ballot in a manner that segregates the processed ballots from exception ballots such that the image can be reviewed and adjudicated by election authorities .

Subparagraph (c) states:

> "Mark the ballot with an identifying mark to facilitate its later identification."

We suggest adding a subparagraph (d) as follows:

> "Prepare, segregate and mark an image copy of the ballot to facilitate its later identification as an exception ballot and as a copy of an original ballot."

Comments on § 3.2.6.2.1 Processing Speed

Subparagraph (a) states that there should be no perceptible delay between voter input and system response. Subparagraph (a) then goes on to give a figure of 250 milliseconds. We believe the sprit of this section can be met with a delay no greater than 750 milliseconds or even 1 second. The reason for this requested change can be found in the time it takes certain steps to be performed in verifying that a vote has been stored correctly, as specified elsewhere in the *Draft VSS Standards*. One can easily imagine a DRE system that stores a completed ballot in memory, makes an image of the ballot on a hard drive and compares those images using error detection and read-after-write techniques that take longer than 250 milliseconds. The performance requirement of no perceptible delay can be met with slightly less stringent requirements of 250 milliseconds.

Comments on § 4.2.3 Software Modularity and Programming

This section provides clear guidelines for modules without defining such "modules." (In later comments, we request that the terms "module" and "procedure" be added to Appendix A Glossary.) The restrictions in the section, while generally aimed at readability and maintainability, can run into contradictions where alternative, yet well-known, definitions are used.

For example, while Visual Basic is anticipated as a high level language in which elections systems can be produced, Visual Basic for Applications uses modules differently than do the standards here. We believe what is intended for the restrictions on "modules" should be restrictions on "procedures." In Visual Basic for Applications, a module consists of a group of procedures having some functional commonality. Thus, it is the procedure that must have a single entry point and it is the procedure, not the module, that should be limited in size pursuant to the guidelines you suggest.[1]

[1] A glossary that points out that "modules" are not what is implied in this section of the *Draft VSS Standards* is found in the Federal Standards FS-1037C. That standard defines module:

> "module: 1. An interchangeable subassembly that constitutes part of, i.e., is integrated into, a larger device or system. (188) 2. In computer programming, a program unit that is discrete and identifiable with respect to compiling, combining with other modules, and loading."

Clearly, because a module can be combined "with other modules" a single entry point to a module is probably not what is intended in the *Draft VSS Standards*.

We believe that is it good practice to restrict procedures to one entry point. We disagree with the restriction on one exit. Often a procedure or function can be written with multiple exits in order to enhance readability and maintainability. Forcing only one exit puts the software designer in a box of having to create if-then-else or do-while constructs that are contrived and artificial. Such arbitrary constraints will render some software harder to maintain and harder to read. We suggest that if a designer builds a procedure with more than one exit, such multiple exits should be documented and explained similarly to the relaxation on module [sic] size that the *Draft VSS Standards* permit. We understand that readable code is an objective of the *Draft VSS Standards*. As the intent of § 4.2.6 (l) points out, multiple levels of indented scope is hard to read and understand. Allowing (and clearly documenting) exit conditions can reduce the number of indented levels.

Comments on § 4.3 Data Quality Assessment

We wonder what the intention of Subparagraph (b) is ("Measure the relative frequency of entry to program units and the frequency of exception conditions."). Does this mean that every subroutine (procedure or function) that is called (consider a simple formatting routine) needs to have the number of times it is entered counted? If so, what purpose does this serve? Perhaps this section meant to count the execution of certain exception processing routines whose monitoring would be useful. If so, we suggest that the types and conditions of "entry into program units" be more specifically described.

Comments on § 4.5.3 In-Process Audit Records

Subparagraph b(4) of this section has the following requirement:

> "For DRE machines at controlled voting locations, the event (and time, if available) of activating and casting each ballot (i.e., each voter's transaction as an event). This data can be compared with the public counter for reconciliation purposes."

We strongly urge the reconsideration of this requirement in the strongest terms. Recording the time of activating and casting each ballot is a method that can be used to identify a voter. Imagine a quiet polling place where a voter checks in at a time when there are no other voters present. The voter votes on a DRE machine and his or her vote is recorded to have occurred at a specific time. If there are no other voters in the polling place at this hypothesized slow time, such a record can be used to identify the voter. Even if there are a few voters in the polling place, such time stamping can be used to narrow down who may have voted for whom. Such time stamping is a major erosion of the secret ballot goals anticipated by voters in a democracy.

Subparagraph (c) of this section requires …[a] summary record of data read-write-verify, parity, or check-sum errors. In many cases such read-write verification data or parity data is simply not available from COTS (commercial off-the-shelf) systems. We respectfully request that if such summary records are required, they only be required where such records can be retrieved from the operating system.

Comments on § 6.2.3 Access Control Measures

While the focus on this section is laudable and is intended to ensure that software used in modern election systems is not tampered with, the terms in which this section is written may not be generally known to the software community. The *Draft VSS Standards* have been meticulous in defining terms where necessary but this high bar has not been met in this section. This reviewing organization cannot find the definition of "security kernal" or "One-end or two-end port protection devices" in the standards nor in the Appendix A Glossary attached to the *Draft VSS Standards*.

A similar concern arises in § **6.5.4.2 Forms of Threats**. With some good reason, the software community has occasionally been criticized for writing in highly technical terms that are not transparent to concerned citizens who are not in that community. This places an appropriate burden on writers who should strive to ensure that all terms are understood. Perhaps the problems of § **6.5.4.2 Forms of Threats** can be solved by including the definition of these terms in the glossary. Good definitions of these terms exist, for example, at the Symantec website (www.symantec.com/securitycheck/glossary.html).

We believe that the *Draft VSS Standards* can achieve a better balance between technical clarity versus election functional clarity. For example, if the well known term "absentee ballot" is defined in the glossary (as it is) shouldn't the term "Trojan horse" be defined as well?

Comments on § 9.2 Testing Scope

The second bullet point of this section states:

> "Operational accuracy in the recording and processing of voting data, as measured by character error rate, for which the maximum acceptable error rate is one in one million characters."

While "character error rate" may be clear in some contexts, we believe it is unclear in this section that has no clear context. We are confident that clarification can be provided, but we think it equally important to introduce another term such as "net character error rate" which we define as the error rate in an information system, including telecommunication transport of data, which is measured as the rate of destination character deviations from the source characters **after error correcting techniques have been applied.** Our urging of this concept makes clear that error correcting techniques can and should be applied to ensure voting data integrity in any part of the vote casting to vote counting process. The acceptable character error rates should be based on net errors: that is to say, remaining errors after well known and reliable error correcting techniques have been applied.

Comments on Volume II § 2.5.10 Appendices

This requirement on documentation requests a "list of module names and variable names." As pointed out above, a high level programming language may group **procedures** into **modules**. We believe the *Draft VSS Standards* should be calling for both module names and procedure names.

Comments on Volume II § 5.4 Source Code Review

Subparagraph E(5) inspects for software recursion (also undefined in the glossary, but a well known software term). We note that Volume I has no prohibition against recursion. While we do not propose that recursion be prohibited (it is a powerful development tool) we wish to point out the inconsistency this test section presents by prohibiting recursion in the code reading phase. Our suggestion is that either recursion is explicitly prohibited or allowed. Our preference is for it to be allowed.

Other comments

While we do not see this in the *Draft VSS Standards,* some commentators have requested that source code be made public. Such a requirement may not be desirable to election system vendors. For any innovation, inventors, developers and vendors in general make investments that they hope will lead to a return on those investments. Making source code public means that anyone can copy that source code and create a system without having made the investments of the creating person or organization. We fear that public source code will stifle the much needed innovation required to move our election systems forward.

Testing laboratories should be allowed to view source code, but persons viewing source code should be prohibited from disclosing any part of the source code. We believe that the testing laboratories should be prohibited from disclosing any proprietary information that comprises a Technical Data Package.

Also, the *Draft VSS Standards* anticipate that certain components of a system will be Commercial Off The Shelf (COTS) products. If the FEC adopts open source, then COTS may not be compliant. In many important cases, including operating systems, compilers, drivers and the like, source code is simply not available.

Respectfully submitted,

Illinois Information Technology Corporation

Sanford J. Morganstein
President